

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 1:19cr59
	)	
DANIEL EVERETTE HALE,	)	
	)	
Defendant	)	

GOVERNMENT’S MOTION *IN LIMINE* TO ALLOW AUTHENTICATION  
AND ADMISSION OF CERTAIN BUSINESS AND ELECTRONIC RECORDS

The United States moves the Court to make pre-trial rulings on the admission of certain business and electronic records that have been certified in accordance with Federal Rule of Evidence 902(11), 902(13), and 902(14). A pre-trial ruling on the admissibility of these documents will reduce the length of trial and conserve the resources of the Court and the parties. Counsel for defendant Hale notified undersigned counsel that the defense generally did not oppose this motion. We file this motion in order to ensure that there is no misunderstanding between the parties as to the authentication of the underlying records.

A. Business Records that are Not Hearsay Pursuant to Fed. R. Evid. 803(6)  
and that Are Self-Authenticating Pursuant to Fed. R. Evid. 902(11)

“To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” Fed. R. Evid. 901(a).

Under Federal Rule of Evidence 902(11), an original or a copy of a domestic record is self-authenticating and requires no extrinsic evidence of authenticity if it meets the requirements of Rule 803(6)(A)-(C), and is accompanied “by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court.”

“Certified domestic records of a regularly conducted activity” may be self-authenticated pursuant to Federal Rule of Evidence 902(11). The records must satisfy the business records requirements of Rule 803(6)(A)-(C), “as shown by a certification of the custodian . . . that complies with a federal statute or a rule prescribed by the Supreme Court.” Fed. R. Evid. 902(11).

Rule 803(6), in turn, provides that business records are admissible if they are accompanied by a certification of their custodian or other qualified person that satisfies three requirements: (A) that the records were “made at or near the time by—or from information transmitted by—someone with knowledge”; (B) that they were “kept in the course of a regularly conducted activity of a business”; and (C) that “making the record was a regular practice of that activity.” *Id.*

The government obtained the following business records during its investigation, and provided those records to the defense during discovery. In each of the following instances, the provider of the records provided a certification of business records, which certifications are attached to this pleading:

1. Government Exhibit 611-C, a certification from Deposit Specialist Patricia Cober, for records of Hale's account at BB&T Bank; and
2. Government Exhibit 620-C, a certification from Coordinator Taneisha Riley, for records from Verizon Wireless of Hale's cell phone account;
3. Government Exhibit 701-A, a certification from Record Custodian Benjamin Paul Kuslits, for Google LLC, for records of Hale's gmail account.

As stated in the attached certificates, the business records sought to be admitted here meet the requirements of Rule 803(6) because they “were made at or near the time – or from information transmitted by – someone with knowledge; “were kept in the course of a regularly conducted activity of a business, organization, occupation, or calling;” and were made as “a regular practice of that activity.” The government has given the defense reasonable written notice

of its intent to offer the evidence that is the subject of this motion and has produced the records to the defense.

The provider records certified pursuant to 902(11), in Government Exhibits 611-C, 620-C, and 701-A, are *prima facie* authentic. See *United States v. Hassan*, 742 F.3d 104, 133 n.25 (4th Cir. 2014) (rejecting as “entirely unpersuasive” the contention that the Facebook and Google certifications were insufficient). The United States requests that the Court rule that these records will be admitted pursuant to Rule 902(11), so that these providers - - BB& T Bank, Verizon Wireless, and Google, LLC - - need not appear at trial.

B. Business Records that are Not Hearsay Pursuant to Fed. R. Evid. 803(6) and 803(8) and that Are Self-Authenticating Pursuant to Fed. R. Evid. 902(4) and (11)

The government also obtained during its investigation, and provided to the defense during discovery, official records filed in public offices as required by law, of regularly conducted activities of agencies of the United States, made at or near the time of the events and conditions contained therein, in accordance with the regular practice of such activities, that complies with the requirements of Rules 902(4) and (11), as certified by the following exhibits, which certifications are attached to this pleading:

1. Government Exhibit 419-A, a certification from Charles Watters, Executive Program Manager of the Freedom of Information and Privacy Act Office, Federal Investigative Services, of the U.S. Office of Personnel Management, for personnel records of Daniel Hale;
2. Government Exhibit 420-A, a certification from Kimberly Reese, Chief of the Records Management Branch for the U.S. Air Force, for personnel records of Daniel Hale maintained by the USAF.
3. Government Exhibit 707, a certification from Tracy Thornton, Branch Chief - Supervisor Adjudicator at NGA, for personnel records of Daniel Hale maintained by NGA;
4. Government Exhibit 708, a certification from Phillip Holland, Chief of Information Security Management at NSA, for personnel records of Daniel Hale maintained by NSA;

5. Government Exhibit 709, a certification from Aaron Mathers, Operations NCO for JSOC, for personnel records of Daniel Hale maintained by JSOC; and

The records that are the subject of the certifications listed above are accompanied by certificates pursuant to Rules 902(4) and (11) and should, accordingly, be admitted as authentic and not hearsay.

- C. Business Records that are Not Hearsay Pursuant to Fed. R. Evid. 803(6) and 803(8), and that Are Self-Authenticating Pursuant to Rules 902(11) and (13)

In 2017, Federal Rules of Evidence 902(13) became effective. Pursuant to this rule, certified records generated by an electronic process or system that produces an accurate result are self-authenticating, removing any need to provide extrinsic evidence of authenticity (such the testimony of a live witness) at a trial or hearing.<sup>1</sup> The records are properly authenticated through a certification satisfying Federal Rules of Evidence 901(11) and 902(13).

In enacting Rule 902(13), the Rules Committee noted that “as with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary.” Fed. R. Evid. 902(13), Advisory Committee’s Note (2017). “It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented.” *Id.*

“The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.”

*Id.* Specifically, Rule 902(13) clarifies that digital evidence “generated by an electronic process

---

<sup>1</sup> Rule 902(13) states, “A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).”

or system that produces an accurate result, as shown by a certification of a qualified person..." is self-authenticating. Fed. R. Evid. 902(13).

The "certification of a qualified person" must comply with the certification requirements of Rule 902(11) or (12), and the proponent of the self-authenticating evidence must provide notice as required by Rule 902(11) to the adverse party before the trial or hearing in which the evidence will be offered. *Id.*

In this case, the government obtained during its investigation, and provided to the defense during discovery, records that were generated by electronic processes or systems that produce accurate results, as shown by Government Exhibit 430, a certification from Stanley K. Robinson, Chief of Investigations for the Counter-Insider Threat Office at the National Geo-Spatial Intelligence Agency ("NGA"). Mr. Robinson's certification, which is attached to this pleading, complies with the requirements of Rule 902(11) and (13), with respect to the following records that were generated by electronic processes or systems at NGA:

- a. badge records with respect to Daniel Hale's physical access to the NGA facility;
- b. personal profile record for NGA employee Daniel Hale;
- c. log-in and lock screen records for Daniel Hale's computer network accounts;
- d. list of documents printed through Daniel Hale's computer user account on NGA's computer system for classified records;
- e. print-outs of 18 binary files generated as a result of documents printed through Daniel Hale's computer user account on NGA's computer system for classified records; and
- f. print-outs of 33 PDFs of binary files described above in subparagraph (e), that were created by opening the binary files in a software application called O&K and a software application called Ghost PCL.

The records that are the subject of Mr. Robinson's certification are records that he - - as a qualified person - - certifies as having been generated by electronic processes or systems that

produce an accurate result. Further, as shown by his certification, they meet the requirements of Federal Rule of Evidences 803(6) and 902(11), in that (a) they were made at or near the time by or from information transmitted by someone with knowledge; (b) they were kept in the course of a regularly conducted activity of an organization; and (C) making the records was a regular practice of that activity. And, notwithstanding the application of Rules 803(6) and 902(11), they are self-authenticating pursuant to Rule 902(13) because they were generated by a reliable electronic process or system. Accordingly, they should be admitted as authentic and not hearsay.

D. Records that Are Self-Authenticating Pursuant to Fed. R. Evid. 902(14)

In 2017, in addition to the new Federal Rule of Evidence 902(13), Federal Rule of Evidence 902(14) also became effective. Under this rule, “[d]ata copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person . . .” constitutes self-authenticating evidence. Fed. R. Evid. 902(14). As with evidence under Rule 902(13), “[a] proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial.” *Id.*, Advisory Committee’s Note (2017).

The government obtained during its investigation, and provided to the defense during discovery, data copied from electronic storage devices, storage media, and files. In each of the following instances, a qualified witness authenticated the particular digital images identified in the following certifications (attached to this pleading), in accordance with the Federal Rules of Evidence, Rule 902(14):

1. Government Exhibit 427, a certification from FBI Information Technology Specialist- Forensic Examiner William Paulemon, with respect to the results of the examination of the Hewlett-Packard hard drive bearing image identifier HQB000210;

2. Government Exhibit 428, a certification from FBI Supervisory Information Technology Specialist- Forensic Examiner Charlotte Baker, with respect to the results of the examination of the Western Digital hard drive bearing image identifier HQB000184; the Samsung Galaxy Note II SCH phone bearing image identifier HQB000162; the 16GB PNY thumb drive bearing image identifier HQB000163; and the DataStick Pro thumb drive, bearing image identifier HQB000165;
3. Government Exhibit 429, a certification from FBI Information Technology Specialist- Forensic Examiner Chad Bayner, with respect to the results of the examination of the hard drives found within the personal computer seized from Hale's home and bearing image identifier HQB000173 and HQB000174.

The certifications listed above establish that each of the certifiers made a complete and accurate image of the devices described in the certifications, and that they were qualified to do so. The records that are the subject of the certifications of the forensic examiners are accompanied by certificates pursuant to Rule 902(14) and, accordingly, should be admitted as authentic.

#### Conclusion

For all of the foregoing reasons, the Court should admit the records by certification and without need for testimony from custodian of records witnesses to authenticate the records.

Respectfully submitted,

G. Zachary Terwilliger  
United States Attorney

By:

/s/

Gordon D. Kromberg  
Assistant United States Attorney  
United States Attorney's Office  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
Phone: 703-299-3700  
Fax: 703-299-3981  
Gordon.kromberg@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that, on November 23, 2020, I electronically filed the foregoing copy of the GOVERNMENT'S MOTION IN LIMINE TO ADMIT CERTAIN BUSINESS RECORDS with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to counsel of record.

By: /s/  
Gordon D. Kromberg  
Assistant United States Attorney  
United States Attorney's Office  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
Phone: 703-299-3700  
Fax: 703-299-3981  
Gordon.kromberg@usdoj.gov